

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE
PLACEMENT CONSUMER PRIVACY
LITIGATION

C.A. 12-MD-2358 (SLR)

This Document Relates to:

**REPLY BRIEF IN SUPPORT OF MOTION TO DISMISS OF DEFENDANTS MEDIA
INNOVATION GROUP, LLC AND WPP PLC FOR FAILURE TO STATE A CLAIM**

OF COUNSEL:

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

Lisa M. Coyle
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 596-9000

June 19, 2013

MORRIS, NICHOLS, ARSHT & TUNNELL LLP
Rodger D. Smith II (#3778)
Regina S.E. Murphy (#5648)
1201 North Market Street, 18th Floor
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
rsmith@mnat.com
rmurphy@mnat.com

*Attorneys for Defendants Media Innovation
Group, LLC and WPP plc*

TABLE OF CONTENTS

	Page
INTRODUCTION	1
ARGUMENT	1
I. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE WIRETAP ACT.....	1
A. Plaintiffs’ Wiretap Act Claim Is Precluded By The Statutory Party Exception.....	1
B. Alternatively, Plaintiffs’ Wiretap Act Claim Is Precluded By The Statutory “Prior Consent” Exception	3
C. Moving Defendants Did Not “Intercept” The “Contents” Of Any Communication.....	4
II. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE STORED COMMUNICATIONS ACT.....	5
A. Plaintiffs Allege No Facility Through Which An ECS Is Provided	5
B. Moving Defendants Did Not Obtain Any Electronic Communications While They Were “In Electronic Storage”.....	7
III. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE CFAA	8
CONCLUSION.....	10

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	8
<i>Callaway Golf Co. v. Dunlop Slazenger Grp. Americas, Inc.</i> , 295 F. Supp. 2d 430 (D. Del. 2003)	7
<i>Chance v. Ave. A, Inc.</i> , 165 F. Supp. 2d 1153 (W.D. Wash. 2001)	6
<i>Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio</i> , Civ. No. 09-2751, 2011 WL 6088611 (E.D. Pa. Dec. 7, 2011)	8
<i>Commw. of Pa. ex rel. Zimmerman v. PepsiCo, Inc.</i> , 836 F.2d 173 (3d Cir. 1988)	6
<i>CoStar Realty Info., Inc. v. Field</i> , 612 F. Supp. 2d 660 (D. Md. 2009)	9
<i>Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz</i> , 793 F. Supp. 2d 311 (D.D.C. 2011)	6
<i>Cousineau v. Microsoft Corp.</i> , No. C11-1438-JCC, slip op. (W.D. Wash June 22, 2012)	6
<i>Craigslist, Inc. v. 3Taps, Inc.</i> , No. CV 12-03816 CRB, 2013 WL 1819999 (N.D. Cal. Apr. 30, 2013)	8
<i>Creative Computing v. Getloaded.com, LLC</i> , 386 F.3d 930 (9th Cir. 2004)	8
<i>Crowley v. Cybersource Corp.</i> , 166 F. Supp. 2d 1263 (N.D. Cal. 2001)	6
<i>Del Vecchio v. Amazon, Inc.</i> , No. C11-366RSL, 2012 WL1997697 (W.D. Wash. June 1, 2012)	9
<i>Ervin & Smith Advert. & Public Relations, Inc. v. Ervin</i> , No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009)	9
<i>Expert Janitorial, LLC v. Williams</i> , No. 3:09-CV-283, 2010 WL 908740 (E.D. Tenn. Mar. 12, 2010)	6

<i>Facebook v. Power Ventures</i> , 844 F. Supp. 2d 1025 (N.D. Cal. Feb. 16, 2012)	8
<i>Freedom Banc Mortg. Servs. Inc. v. O’Harra</i> , No. 2:11-cv-01073, 2012 WL 3862209 (S.D. Ohio Sept. 5, 2012)	6
<i>Garcia v. City of Laredo</i> , 702 F.3d 788 (5th Cir. 2012)	6
<i>In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Serv. Account/User Name [xxxxxxxxxxx@xxx.com]</i> , 396 F. Supp. 2d 45 (D. Mass. 2005)	5
<i>In re Doubleclick Inc. Privacy Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001)	3, 7, 9
<i>In re Intuit Privacy Litig.</i> , 138 F. Supp. 2d 1272 (C.D. Cal. 2001)	6
<i>In re iPhone Application Litig.</i> , 844 F. Supp. 2d 1040 (N.D. Cal. 2012)	2, 6, 9
<i>U.S. v. Allen</i> , 53 M.J. 402 (C.A.A.F. 2000)	4
<i>U.S. v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	5
<i>U.S. v. Polizzi</i> , 549 F. Supp. 2d 308 (E.D.N.Y. 2008)	4
<i>United Factory Furnishings v. Alterwitz</i> , No. 2:12-cv-00059, 2012 WL 2138115 (D. Nev. June. 13, 2012)	9
<i>Victaulic Co. v. Tieman</i> , 499 F.3d 227 (3d Cir. 2007)	3

STATUTES

18 U.S.C. § 1030(e)(6)	8
18 U.S.C. § 2510(4)	4
18 U.S.C. § 2710(17)	7

INTRODUCTION¹

Throughout their Opposition Brief, Plaintiffs mistakenly assume that merely invoking and repeating certain words such as “hacking” and “tricking” relieves them of the obligation to plead facts that, if true, show that Moving Defendants’ violated the statutes on which Plaintiffs base their claims. It does not. When assumed true and disentangled from unsupported conclusions and inflammatory rhetoric, the *facts* alleged in the CAC are that:

- Plaintiffs requested ads from, and in the process voluntarily sent information to, Moving Defendants whether or not Moving Defendants set a cookie on their browser, and thus Moving Defendants did not “intercept” any information;
- Any cookies set by Moving Defendants on Plaintiffs’ browsers were set by interacting with Plaintiffs’ browsers in precisely the way they were designed to function, and thus were not “unauthorized”;
- Moving Defendants received neither PII nor the “contents” of any of Plaintiffs’ communications; and
- Plaintiffs suffered no loss whatsoever as a result of Moving Defendants’ alleged conduct.

These facts do not meet the requirements of the Wiretap Act, SCA or CFAA, and thus Plaintiffs’ claims against Moving Defendants should be dismissed.

ARGUMENT

I. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE WIRETAP ACT

A. Plaintiffs’ Wiretap Act Claim Is Precluded By The Statutory Party Exception

Plaintiffs allege that their browsers sent the Browser-Generated Information directly to Moving Defendants in connection with requests for ads. (CAC ¶ 41.) This allegation makes

¹ Capitalized terms not defined herein have the meanings ascribed to them in the Moving Defendants’ opening brief (the “Opening Brief”). Plaintiffs’ brief in opposition to the Moving Defendants’ motion to dismiss is referred to herein as the “Opposition Brief” or “Opp. Br.,” and Plaintiffs’ brief in opposition to defendant Vibrant Media, Inc.’s motion to dismiss, is referred to herein as the “Vibrant Brief” or “Vibrant Br.”

Moving Defendants, by definition, parties to the alleged communication of that information, and renders the Wiretap Act inapplicable to that communication. (*See* Opening Br. at 5-7.) In response, Plaintiffs claim they did not “intend[]” for Moving Defendants to be parties to their communications. (Opp. Br. at 4.) But nothing in the Wiretap Act suggests that the applicability of the “party exception” hinges on the communicating party’s subjective intent – something that the recipient could not possibly know.

In re iPhone, on which Plaintiffs rely, is not to the contrary, as plaintiffs there took no affirmative steps to send the defendant information. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1050-51 (N.D. Cal. 2012) (“*iPhone II*”). Rather, the defendant sought to rely on *its own actions* – it had designed its software to enable the collection of information to which the plaintiffs objected – in invoking the party exception. *Id.* Here, in stark contrast, Moving Defendants did not “design” Plaintiffs’ browsers or cause those browsers to visit websites that in turn led them to request ads from Moving Defendants. Moreover, Plaintiffs argue that Moving Defendants’ alleged improper setting of cookies “trick[ed]” Plaintiffs’ browsers into communicating directly with Moving Defendants. (Opp. Br. at 3.) This argument, however, ignores the allegations in the CAC that Plaintiffs sent the Browser-Generated Information to Moving Defendants each time they visited a website on which Moving Defendants serve ads *regardless of whether Moving Defendants had set a cookie on the browsers.* (CAC ¶ 41.) Moving Defendants’ alleged post-receipt “associat[ion]” of Browser-Generated Information received from a browser on different occasions, which Plaintiffs say the cookies enabled, thus does not alter Moving Defendants’ status as alleged parties to the initial communication. (*Id.*)

B. Alternatively, Plaintiffs’ Wiretap Act Claim Is Precluded By The Statutory “Prior Consent” Exception

Even under the theory (contradicted by Plaintiffs’ allegations) that Moving Defendants acquired the Browser-Generated Information not directly from Plaintiffs, but while it was being sent to websites Plaintiffs visited, the Wiretap Act claim would fail because any website displaying ads served by Moving Defendants necessarily consented to Moving Defendants’ receipt of Browser-Generated Information. *See In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).² Regardless of any after-the-fact statements the owners of these websites may have made, it would be “implausible to infer” that they “ha[d] not authorized [Moving Defendants’] access” because “the very reason clients hire [ad-serving companies]” is to have ads delivered to their webpages. *Id.* at 510.³ Plaintiffs attempt to distinguish *Doubleclick* based on the court’s observation that plaintiffs could have “configur[ed] their browsers to prevent any cookies from being deposited.” *Id.* at 504-05. Plaintiffs argue that their browsers were configured “to do just that,” but that cookies were still set. (Opp. Br. at 5.)

This argument is refuted by the CAC, which alleges that: (i) the Partial Allowance Setting prevented *some* cookies and permitted others; and (ii) the cookies were set in accordance with an “exception” to the general exclusion of third party cookies. (CAC ¶¶ 69-73, 76-77.) Moreover, documents incorporated by reference into the CAC confirm that, as in *In re Doubleclick*, Plaintiffs could have “easily and at no cost prevent[ed] [Moving Defendants] from

² Plaintiffs’ argument that consent is an affirmative defense and not a proper basis for dismissal is meritless because the facts giving rise to the defense appear on the face of the CAC. *Victaulic Co. v. Tieman*, 499 F.3d 227, 234-35 (3d Cir. 2007); *see also In re Doubleclick*, 154 F. Supp. 2d at 510, 514.

³ Nor does the CAC support the assertion that the Moving Defendants “exceeded any consent they had to place an ad,” as it would be equally implausible to infer that a website authorized the Moving Defendants to serve ads but not to receive information necessary to do so. (Opp. Br. at 5, n.5); *see In re Doubleclick*, 154 F. Supp. 2d at 510.

collecting information.” (*See Safari Features, Security and Privacy*, Reply Declaration of Lisa M. Coyle, dated June 19, 2013 Ex. B (users can “customize cookie settings” and “prevent[] the websites [they] visit. . . from . . . access[ing] cookies . . . already stored on . . . computer”); *cf.* CAC ¶ 69 n.51.)

C. Moving Defendants Did Not “Intercept” The “Contents” Of Any Communication

Plaintiffs’ Wiretap Act claim also fails because they do not allege that Moving Defendants “intercept[ed]” the “contents” of their communications. Plaintiffs argue that Moving Defendants acquired URLs of websites visited by Plaintiffs (which Plaintiffs say are contents) by using their “computers and web servers to secretly embed code [*i.e.*, cookies] that fooled Plaintiffs’ web browsers into sending [the URLs] to [Moving] Defendants.” (Opp. Br. at 6 n.6.) The allegations in the CAC, however, are that Plaintiffs’ browsers sent the URLs to Moving Defendants every time Plaintiffs requested an ad – *regardless of whether or not Moving Defendants had set a cookie*. (CAC ¶ 41.) Thus, any acquisition of URLs by Moving Defendants was not accomplished by means of any cookies Moving Defendants may have set, and hence was not “through the use of any electronic, mechanical, or other device,” as it must be to constitute an “intercept[ion]” under the Wiretap Act. 18 U.S.C. § 2510(4).⁴

Moreover, URLs are not contents. *See U.S. v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008) (“[n]o expectation of privacy exists for . . . a user’s Internet search history”), *vacated on other grounds by* 564 F.3d 142 (2d Cir. 2009); *U.S. v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (“log identifying . . . detailed internet address of sites accessed by appellant” were mere “transactional records” not “communications”). Plaintiffs’ argument to the contrary

⁴ Any objection to the alleged post-receipt “associat[ion]” of this information is thus an objection to the alleged *use* of information lawfully received – conduct not governed by the Wiretap Act. (*See* Part I.A, *supra*.)

is based on a footnote in a nonbinding case suggesting that “[s]urveillance techniques that enable the government to determine . . . [the] URL of the pages visited *might* be more constitutionally problematic” than those revealing IP addresses. *U.S. v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008).⁵ This hypothetical statement, however, is *dicta*, and even if it were not, *Forrester* is inapposite, as it involved targeted surveillance of *a specific person*, not the alleged receipt of *anonymous* information. (See Opening Br. at 16) (discussing CAC’s lack of allegations showing that Moving Defendants received PII). A collection of URLs visited by “browser X” does not reveal the same information as a specific, identifiable individual’s web browsing history.⁶

II. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE STORED COMMUNICATIONS ACT⁷

A. Plaintiffs Allege No Facility Through Which An ECS Is Provided

Although the CAC alleged that Plaintiffs’ browsers provided an ECS through browser managed files that were “facilities” under the SCA, Plaintiffs now say that their computers, browsers and browser managed files are *all* “facilities” through which an ECS – “internet service”

⁵ All emphasis added unless otherwise stated.

⁶ The other case on which Plaintiffs rely is a non-binding decision by a magistrate judge who “acknowledged [his] dearth of technological savvy” and admitted that he had not “had the luxury of studying the problem thoroughly” before ruling, discussing in *dicta* hypothetical issues that *might* arise if the government had requested an order authorizing the collection of URLs, which it had not. *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Serv. Account/User Name [xxxxxxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

⁷ Plaintiffs do not plead facts showing that: (i) the alleged cookie setting was unauthorized; (ii) the Moving Defendants’ alleged receipt of any Cookie Values was unauthorized; and (iii) the Moving Defendants received Browser Generated Information through the alleged cookie-setting. (Opening Br. at 9-11.) In response to these arguments, Plaintiffs merely repeat their mantra that Moving Defendants used “trickery” to set cookies that Plaintiffs had set their browsers to block, enabling Moving Defendants to receive unspecified “additional information.” (Opp. Br. at 8-10, 12-13.) As discussed *supra*, these conclusory statements are not adequate substitutes for facts showing that the SCA’s requirements have been met. (See Parts I.A & B, *supra*.)

– is provided. (*Compare* CAC ¶¶ 216-18 with Vibrant Br. at 5.)⁸ The “facilities that the SCA is designed to protect,” however, “are facilities that are *operated by [ECS] providers.*” *Freedom Banc Mortg. Servs. Inc. v. O’Harra*, No. 2:11-cv-01073, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012). Because Plaintiffs themselves – not their internet service providers – “operate” their own devices, software and files, those devices, software, and files cannot be “facilities.”

Indeed, Plaintiffs’ argument has been overwhelmingly rejected by courts taking “a close[] analytical look” at the issue. *See, e.g., Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001) (interpreting “facility” to include user’s device “would render other parts of the [SCA] illogical”).⁹ The few decisions concluding that personal devices can be facilities are against the overwhelming weight of authority, “provide little analysis,” and should not be followed. *iPhone II*, 844 F. Supp. 2d at 1058 (disagreeing with *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272 (C.D. Cal. 2001), and *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740 (E.D. Tenn. Mar. 12, 2010)); *see also Cousineau v. Microsoft Corp.*, No. C11-1438-JCC, slip op. (W.D. Wash June 22, 2012) (failed to consider weight of authority).¹⁰

⁸ Plaintiffs’ new theory need not be considered, as they may not amend the CAC through briefing. *Commw. of Pa. ex rel. Zimmerman v. PepsiCo, Inc.*, 836 F.2d 173, 181 (3d Cir. 1988) (internal quotation marks and citation omitted).

⁹ *See also Garcia v. City of Laredo*, 702 F.3d 788, 788 (5th Cir. 2012) (reviewing legislative history and case law and concluding cell phones are not “facilities” under SCA). Plaintiffs argue that *Garcia* is distinguishable because Plaintiffs allege that the files were stored by the Moving Defendants rather than the users, but this distinction has no bearing on *Garcia*’s holding that the SCA protects facilities operated by internet service providers. *Id.* That *Garcia* was decided on summary judgment is equally unhelpful to Plaintiffs, as the court decided the issue as a matter of law, and Plaintiffs do not allege they are ECS providers. *Id.* at 793.

¹⁰ Nor are Plaintiffs helped by the other cases on which they rely. *See Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334 (D.D.C. 2011) (access to “physical client-side computer” *not* actionable under SCA); *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (though “it is *possible* to conclude that modern computers . . . are facilities covered under the Act . . . the subsequent implications of *this rather strained interpretation* . . . are fatal to [plaintiffs’] cause of action”). Finally, Plaintiffs’ effort to

B. Moving Defendants Did Not Obtain Any Electronic Communications While They Were “In Electronic Storage”

Plaintiffs’ attempts to distinguish the weight of authority holding that electronic communications stored on personal computers are not “in electronic storage” are similarly unavailing. First, the only information allegedly obtained from the purportedly “temporarily stored” cookies was the Cookie Values and, “to the extent cookie identification numbers are electronic communications *at all*,” they belong not to Plaintiffs, but to Moving Defendants. *In re Doubleclick*, 154 F. Supp. 2d at 511-13. Moreover, Plaintiffs’ argument that the cookies were “temporarily stored” is contradicted by the CAC, which states that the cookies were “persistent” and “could stay on a user’s device for years.” (*Compare* Opp. Br. at 11 with CAC ¶ 39(a).)¹¹

Plaintiffs next attack a straw man by arguing that the relevant information need not have been “in transmission.” (Opp. Br. at 11-12.) Moving Defendants argue that the statute requires the information to have been in “*intermediate*” storage – *not* “in transmission” – and Plaintiffs do not allege that it was. (Opening Br. at 14); *see* 18 U.S.C. § 2710(17). Finally, Plaintiffs make the incongruous argument that they are entitled to plead “in the alternative” that their information was accessed (i) while in storage on their devices, *and* (ii) while in transit to first-party websites. (Opp. Br. at 12 n.11; CAC ¶¶ 41, 208.) Although Plaintiffs “may plead *alternative theories of relief* based on the *same set of facts*,” if Rule 11 is to have any meaning at all, they may not plead *mutually exclusive facts*. *See Callaway Golf Co. v. Dunlop Slazenger Grp. Americas, Inc.*, 295 F. Supp. 2d 430, 438 (D. Del. 2003).

convert the statutory definitions of “ECS” and “facility” into factual issues requiring discovery must fail, as the Moving Defendants’ arguments are premised on the assumption, for purposes of this motion only, that the CAC’s factual allegations are true. (Opp. Br. at 10.)

¹¹ Plaintiffs argue that the other cases the Moving Defendants cite are inapposite because they involved access to emails, but do not explain why this fact is relevant. (Opp. Br. at 11.)

III. PLAINTIFFS FAIL TO STATE A CLAIM UNDER THE CFAA

Plaintiffs contend that merely because Moving Defendants allegedly use data such as the Browser-Generated Information in connection with their business, there is a plausible inference that they “knowingly hacked [Plaintiffs’] Safari default setting” to obtain such data. (Opp Br. at 12.) This is precisely the type of *non sequitur* that *Twombly* held should not be countenanced on a Rule 12(b)(6) motion. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007) (where factual allegations are equally consistent with legal and illegal behavior, complaint “stops short of the line between possibility and plausibility.”). In defense of their CFAA claim, however, Plaintiffs offer little more than this astonishing, and legally insufficient, assertion.

First, for all the reasons previously discussed, Plaintiffs allege no facts supporting their assertion that Moving Defendants accessed Plaintiffs’ computers “without authorization” or “used [authorized] access . . . to obtain or alter information” that they were “not entitled to so obtain or alter.” 18 U.S.C. § 1030(e)(6); *see* Parts I.A & I.B, *supra*. Accordingly, Plaintiffs fail to plead a violation of § 1030, as they must to assert a private right of action under the CFAA.¹² Moreover, Plaintiffs’ contention that Moving Defendants rely on an overly narrow interpretation of the term “loss,” is both inaccurate and irrelevant. (Opp. Br. at 16-18.)¹³ The cases Plaintiffs

¹² Plaintiffs rely on *Craigslist, Inc. v. 3Taps, Inc.* and *Facebook v. Power Ventures* to argue that the alleged cookie-setting “circumvented” technological barriers and thus was a *per se* violation of the CFAA. (Opp. Br. at 13 (discussing *Craigslist*, No. CV 12-03816 CRB, 2013 WL 1819999, at *4 (N.D. Cal. Apr. 30, 2013) and *Facebook*, 844 F. Supp. 2d 1025, 1037 (N.D. Cal. Feb. 16, 2012)).) Both cases are distinguishable, as plaintiffs alleged that they had issued cease and desist letters to, and blocked the IP addresses of, the defendant, facts not alleged here.

¹³ “Loss” under the CFAA is limited to “the cost of remedial measures taken to investigate or repair the damage to the . . . computer,” and “lost revenue resulting from . . . [the] inability to utilize the computer.” *Clinton Plumbing & Heating of Trenton, Inc. v. Ciaccio*, Civ. No. 09-2751, 2011 WL 6088611, at *5 (E.D. Pa. Dec. 7, 2011); *see also Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930, 935 (9th Cir. 2004) (defining economic damages as money or property “impaired in value” or “lost” or money spent “to restore or maintain some aspect of the business affected by a violation”).

cite for a broader interpretation involved specific allegations that plaintiffs *themselves* incurred actual costs or lost actual revenue. *See, e.g., United Factory Furnishings v. Alterwitz*, No. 2:12-cv-00059, 2012 WL 2138115 (D. Nev. June. 13, 2012) (plaintiffs conducted damage assessment and obtained mirror image of computer equipment).¹⁴ Plaintiffs’ “loss” allegations, by contrast, are limited to the sweeping generalization (based on studies, newspaper articles, and the purported business practices of companies other than Moving Defendants) that *some* PII can have value to *some* people in *some* circumstances. (*See, e.g.,* CAC ¶¶ 56 (study of “value that 180 [unidentified] Internet users placed on keeping personal data secure”); *id.* ¶ 61 (Financial Times article states Facebook IPO “could value the company at up to \$100 [billion]”).) Courts consistently reject such allegations because they show no actual detriment *to plaintiffs*.¹⁵

Finally, Plaintiffs incorporate by reference their argument in Section IV.C.5 of the Vibrant Brief regarding aggregation of losses under the CFAA. This argument fails for all of the reasons set forth in the Opening Brief, as well as in Section II.B of Vibrant’s reply brief, which Moving Defendants hereby incorporate by reference.

¹⁴ *See also CoStar Realty Info., Inc. v. Field*, 612 F. Supp. 2d 660, 674 (D. Md. 2009) (lost license fee revenue); *Ervin & Smith Advert. & Public Relations, Inc. v. Ervin*, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009) (theft of proprietary information resulting in lost revenue).

¹⁵ *See, e.g., Del Vecchio v. Amazon, Inc.*, No. C11-366RSL, 2012 WL1997697, at *4 (W.D. Wash. June 1, 2012) (“it is not enough to allege that [plaintiffs’] information has value to [the defendants]; the term ‘loss’ requires that plaintiffs suffer a detriment”); *In re DoubleClick*, 154 F. Supp. 2d at 525 (“[d]emographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers,” and “*the value of its collection has never been considered an economic loss to the subject*”); *iPhone II*, 844 F. Supp. 2d at 1068 (holding allegations of loss arising from the collection or use of, or access to, personal information insufficient to support CFAA claim).

CONCLUSION

For all of the foregoing reasons, as well as those previously stated, Moving Defendants respectfully request that the Court dismiss all of the claims asserted against Moving Defendants in the CAC.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Rodger D. Smith II

OF COUNSEL:

Douglas H. Meal
ROPES & GRAY LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
(617) 951-7000

Lisa M. Coyle
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
(212) 596-9000

June 19, 2013

7306404

Rodger D. Smith II (#3778)
Regina S.E. Murphy (#5648)
1201 North Market Street, 18th Floor
P.O. Box 1347
Wilmington, DE 19899-1347
(302) 658-9200
rsmith@mnat.com
rmurphy@mnat.com

*Attorneys for Defendants Media Innovation
Group, LLC and WPP plc*

CERTIFICATE OF SERVICE

I hereby certify that on June 19, 2013, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on June 19, 2013, upon the following in the manner indicated:

Charles Slanina, Esquire
David L. Finger, Esquire
FINGER & SLANINA, LLC
One Commerce Center
1201 North Orange Street, 7th Floor
*Steering Committee Member and Liaison
Counsel for Plaintiffs*

VIA ELECTRONIC MAIL

Stephen G. Grygiel, Esquire
KEEFE BARTELS
170 Monmouth Street
Red Bank, NJ 07701
*Interim Lead Counsel for the Putative Plaintiff
Class*

VIA ELECTRONIC MAIL

Brian Russell Strange, Esquire
STRANGE & CARPENTER
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
*Interim Lead Counsel for the Putative Plaintiff
Class*

VIA ELECTRONIC MAIL

James Frickleton, Esquire
BARTIMUS, FRICKLETON, ROBERTSON
& GORNY-LEAWOOD
11150 Overbrook Road, Suite 200
Leawood, KS 66211
*Interim Lead Counsel for the Putative Plaintiff
Class*

VIA ELECTRONIC MAIL

Barry Eichen, Esquire
EICHEN, CRUTCHLOW, ZASLOW & MCELROY LLP
40 Ethel Road
Edison, NJ 08817
Plaintiffs' Steering Committee Member

VIA ELECTRONIC MAIL

William H. Murphy, Jr., Esquire
MURPHY P.A.
One South Street, Suite 2300
Baltimore, MD 21202
Plaintiffs' Steering Committee Member

VIA ELECTRONIC MAIL

Mark Bryant, Esquire
BRYANT LAW CENTER, PSA
601 Washington Street
P.O. Box 1876
Paducah, KY 42002-1876
*Counsel for Plaintiff William G. Gourley and
Plaintiffs' Steering Committee Member*

VIA ELECTRONIC MAIL

Jonathan Shub, Esquire
SEEGER WEISS LLP
1515 Market Street, Suite 1380
Philadelphia, PA 19102
*Counsel for Plaintiff Lynne Krause and
Plaintiffs' Steering Committee Member*

VIA ELECTRONIC MAIL

Jay Barnes, Esquire
BARNES & ASSOCIATES
219 East Dunklin Street
Jefferson City, MO 65101
Plaintiffs' Steering Committee Member

VIA ELECTRONIC MAIL

Seth D. Rigrodsky, Esquire
Brian D. Long, Esquire
Gina M. Serra, Esquire
RIGRODSKY & LONG, P.A.
2 Righter Parkway, Suite 120
Wilmington, DE 19801
*Council for Proposed Intervening Plaintiffs
Daniel Mazzone, Michelle Kuswanto, Michael
Frohberg and Andy Wu*

VIA ELECTRONIC MAIL

Kim E. Richman, Esquire
Michael R. Reese, Esquire
George Granade, Esquire
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Council for Proposed Intervening Plaintiffs
Daniel Mazzone, Michelle Kuswanto, Michael
Frohberg and Andy Wu

VIA ELECTRONIC MAIL

Sanford P. Dumain, Esquire
Adam Bobkin, Esquire
Melissa Clark, Esquire
Leigh Smith, Esquire
MILBERG LLP
One Penn Plaza
New York, NY 10119
Council for Proposed Intervening Plaintiffs
Daniel Mazzone, Michelle Kuswanto, Michael
Frohberg and Andy Wu

VIA ELECTRONIC MAIL

David Azar, Esquire
MILBERG LLP
300 South Grand Avenue, Suite 3900
Los Angeles, CA 90071
Council for Proposed Intervening Plaintiffs
Daniel Mazzone, Michelle Kuswanto, Michael
Frohberg and Andy Wu

VIA ELECTRONIC MAIL

Kelly E. Farnan, Esquire
Rudolf Koch, Esquire
Travis S. Hunter, Esquire
RICHARDS, LAYTON & FINGER P.A.
920 North King Street
Wilmington, Delaware 19801
Attorneys for Defendant Vibrant Media Inc.

VIA ELECTRONIC MAIL

Edward P. Boyle, Esquire
David N. Cinotti, Esquire
Joeann E. Walker, Esquire
VENABLE LLP
1270 Avenue of the Americas, 24th Floor
New York, NY 10020
Attorneys for Defendant Vibrant Media Inc.

VIA ELECTRONIC MAIL

Anthony J. Weibell, Esquire
WILSON SONSINI GOODRICH & ROSATI
650 Page Mill Road
Palo Alto, CA 94304-1050
Attorneys for Defendant Google Inc.

VIA ELECTRONIC MAIL

Carol Lynn Thompson, Esquire
SIDLEY AUSTIN LLP
555 California Street, 20th Floor
San Francisco, CA 94104
Attorneys for Defendant Pointroll Inc.

VIA ELECTRONIC MAIL

/s/ Rodger D. Smith II

Rodger D. Smith II (#3778)